5

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/007,859	11/13/2001	Mark C. Astley	GB920010085US1	7123

25259 7590 04/04/2007

IBM CORPORATION
3039 CORNWALLIS RD.
DEPT. T81 / B503, PO BOX 12195
REASEARCH TRIANGLE PARK, NC 27709

EXAMINER	
TOLENTINO, RODERICK	
ART UNIT	**PAPER NUMBER**
2134	

SHORTENED STATUTORY PERIOD OF RESPONSE	NOTIFICATION DATE	DELIVERY MODE
3 MONTHS	04/04/2007	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Notice of this Office communication was sent electronically on the above-indicated "Notification Date" and has a shortened statutory period for reply of 3 MONTHS from 04/04/2007.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

RSWIPLAW@us.ibm.com

Office Action Summary	Application No.	Applicant(s)	
	10/007,859	ASTLEY ET AL.	
	Examiner	Art Unit	
	Roderick Tolentino	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *01/08/2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-16* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-16* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *11/13/2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1 – 16 are pending.

Continued Examination Under 37 CFR 1.114

2. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 01/16/2007 has been entered.

Response to Arguments

3. Applicant's arguments with respect to claims 1 – 16, have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

5. Claims 1, 9 and 12 – 15 are rejected under 35 U.S.C. 102(b) as being anticipated by Gray U.S. Patent No. (5,884,497).

6. As per claims 1 and 12 – 15, Gray discloses a process at the client data processing system applying the cipher function to the client password, which corresponds to the stored cipher-protected client password, thereby to generate a cipher-protected client password, which is equivalent to the stored cipher-protected client password (Gray, Col. 5 Lines 29 – 40, encrypted passwords), and performing an authentication check using the client data processing system's cipher-protected client password and the server data processing system's stored cipher-protected client password as a shared secret for said authentication check (Gray, Col. 5 Lines 29 – 40, compares to check validity of passwords) the authentication check is adapted to be performed without having the client password in a cleartext format on the server data processing system (Gray, Col. 5 Lines 29 – 40, compares the encrypted passwords) wherein the authentication method is adapted to function without additional software infrastructure (Gray, Col. 5 Lines 29 – 40, no external software needed).

7. As per claim 9 Gray discloses the server processing system's password repository is preferably integrated within the operating system of the server data processing system (Gray, Col. 6 Lines 9 – 21, OS works with verification system of passwords thus accessing all passwords associated to the system).

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claims 2 and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gray U.S. Patent No. (5,884,497) in view of Boyko et al. U.S. Patent No. (7,047,408).

10. As per claim 2, Gray fails to teach an authentication check includes performing a mutual challenge-response authentication protocol check. However, in an analogous art Jablon teaches an authentication check includes performing a mutual challenge-response authentication protocol check (Boyko, Col. 3 Lines 24 – 36).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use Boyko's secure mutual network authentication with Gray's apparatus for providing an authentication system, because it offers the advantage of being a more secure.

11. As per claim 16, Davis as modified teaches generating a cipher-protected client password by applying said first cipher function to the client's password, thereby to provide the client and server processes with a shared secret (Boyko, Col. 3 Lines 24 – 36), generating a client response and counter-challenge to the server challenge, the client response and counter-challenge including a message authentication code computed using the cipher-protected client password (Boyko, Col. 3 Lines 24 – 36),

forwarding the client response and counter-challenge to the server process ((Boyko, Col. 3 Lines 24 – 36) receiving the forwarded server response; generating an anticipated server response and comparing the received and anticipated server responses to determine whether they match; and in response to a positive match, confirming successful authentication (Boyko, Col. 3 Lines 24 – 36).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use Boyko's secure mutual network authentication with Gray's apparatus for providing an authentication system, because it offers the advantage of being a more secure.

12. Claim 3 is rejected under 35 U.S.C. 103(a) as being unpatentable over Gray U.S. Patent No. (5,884,497) in view of Patzer et al. U.S. Patent No. (6,732,270).

13. As per claim 3, Gray fails to teach the cipher function is an encryption algorithm wherein the cipher-protected client password comprises a salt and a character string. However, in an analogous art Patzer teaches the cipher function is an encryption algorithm wherein the cipher-protected client password comprises a salt and a character string (Patzer, Col. 4 Lines 18 – 31).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use Patzer's method to authenticate a network access server to an authentication server with Gray's apparatus for providing an authentication system, because it offers the advantage of protecting against imposter clients (Patzer, Col.2 Lines 16 – 20).

14. Claims 6 – 8 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gray U.S. Patent No. (5,884,497) in view of Davis et al. U.S. Patent No. (6,064,736).

15. As per claim 6, Gray fails to teach a hash function. However, in an analogous art Davis teaches a hash function (Davis, Col. 4, Lines 50 – 52).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use Davis' password verification method and system with Gray's apparatus for providing an authentication system, because it offers the advantage of protecting against unwanted users (Davis, Col. 2 Lines 15 – 26).

16. As per claim 7,Gray as modified teaches a process at the server data processing system retrieving from the repository the respective token for a stored cipher-protected client password, and transmitting the token to a client data processing system (Davis, Col. 5, Lines 11 – 14) and the process at the client data processing system applying the cipher function to the combination of the transmitted token and the client password which corresponds to the stored cipher-protected client password, thereby to generate the equivalent cipher-protected client password for use as a shared secret (Davis, Col. 5, Lines 18 – 31).

17. As per claim 8 Gray as modified teaches the token is a random number (Davis, Col. 5, Lines 11 – 13, salt).

18. Claims 4, 5 and10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gray U.S. Patent No. (5,884,497) in view of Yatsukawa U.S. Patent No. (6,148,404).

19. As per claim 4, Gray fail to teach an authentication check comprises generating a common secret session key at both the client and server data processing systems, using the generated encrypted client password at the client and the stored encrypted client password at the server, and using this common secret session key in a mutual challenge-response authentication protocol. However, Yatsukawa teaches an authentication check comprises generating a common secret session key at both the client and server data processing systems, using the generated encrypted client password at the client and the stored encrypted client password at the server, and using this common secret session key in a mutual challenge-response authentication protocol (Yatsukawa, Col. 19, Lines 62 – 67).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to us Yatsukawa's common session-key with Gray's apparatus for providing an authentication system, because it offers the advantage of confidentiality by limiting the chance of leakage of information between client and server along with unauthorized intrusion (Yatsukawa, Col. 1 Lines 35 – 42).

20. As per claim 5, Gray teaches a secret session key is generated by applying a cipher function to each of the generated encrypted client password at the client and the stored encrypted client password at the server (Yatsukawa, Col. 3, Lines 52 – 55).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to us Yatsukawa's common session-key with Gray's apparatus for providing an authentication system, because it offers the advantage of confidentiality by limiting the chance of leakage of information between client and server along with unauthorized intrusion (Yatsukawa, Col. 1 Lines 35 – 42).

21. As per claim 10, Gray as modified teaches the operating system is an operating system conforming to the UNIX operating system standard or derived from a UNIX conforming system (Yatsukawa, Col. 19, Lines 3 – 6).

22. Claim 11 is rejected under 35 U.S.C. 103(a) as being unpatentable over Gray U.S. Patent No. (5,884,497) and Yatsukawa U.S. Patent No. (6,148,404), as applied to claim 10

23. As per claim 11, Gray fails to teach the encryption algorithm is provided by the UNIX crypt() function. However, in an analogous art Davis teaches the encryption algorithm is provided by the UNIX crypt() function (Davis, Col. 5, Lines 13 – 16).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use Davis' password verification method and system with Gray's apparatus for providing an authentication system, because it offers the advantage of protecting against unwanted users (Davis, Col. 2 Lines 15 – 26).

Conclusion

24. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Roderick Tolentino whose telephone number is (571) 272-2661. The examiner can normally be reached on 8:00am - 5:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Roderick Tolentino
Examiner
Art Unit 2134

KAMBIZ ZAND
PRIMARY EXAMINER

Roderick Tolentino